

AD-A074 614

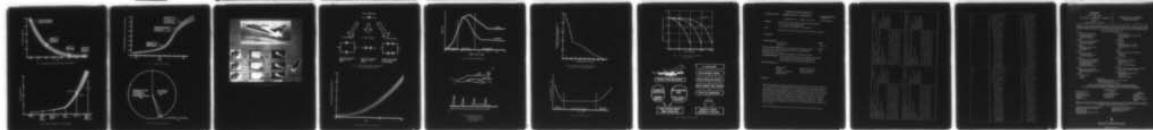
ADVISORY GROUP FOR AEROSPACE RESEARCH AND DEVELOPMENT--ETC F/6 1/4
INTEGRITY IN ELECTRONIC FLIGHT CONTROL SYSTEMS.(U)
JUL 79 P R KURZHALS, R ONKEN

UNCLASSIFIED AGARD-AR-136

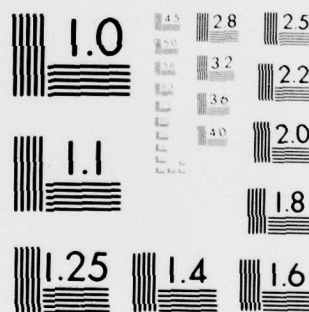
NL

| OF |

AD
A074614



END
DATE
FILMED
11-79
DDC



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

12

AGARD-AR-136

AGARD-AR-136

AGARD

ADVISORY GROUP FOR AEROSPACE RESEARCH & DEVELOPMENT

7 RUE ANCELLE 92200 NEUILLY SUR SEINE FRANCE

AD A U 7 4 6 1 4

LEVEL

AGARD ADVISORY REPORT No. 136

Integrity in Electronic Flight Control Systems

This document has been approved
for public release and sale; its
distribution is unlimited.

DDC
OCT 3 1979
E/

DDC FILE COPY

NORTH ATLANTIC TREATY ORGANIZATION



DISTRIBUTION AND AVAILABILITY
ON BACK COVER

79 10 02 012

NORTH ATLANTIC TREATY ORGANIZATION
ADVISORY GROUP FOR AEROSPACE RESEARCH AND DEVELOPMENT
(ORGANISATION DU TRAITE DE L'ATLANTIQUE NORD)

12 22

9 Advisory report
11 Jul 79

AGARD Advisory Report No.136

6 INTEGRITY IN ELECTRONIC FLIGHT CONTROL SYSTEMS

by

10 Dr P. R. Kurzhaas, R. Onken
Director

Guidance Control and Information Systems Division
National Aeronautics and Space Administration
Washington, DC 20546
USA

and

Dr Ing R. Onken
DFVLR
Institut für Flugführung
Flughafen
D-3300 Braunschweig

DDC
RECEIVED
OCT 3 1978

This Advisory Report provides an overview of major considerations in the design and implementation of reliable electronic flight control systems. Associated material was drawn from AGARDograph AG-224 "Integrity in electronic flight control systems" and other recent AGARD publications on the subject.

This document has been approved for public release and sale; its distribution is unlimited.

This Advisory Report was sponsored by the Guidance and Control Panel of AGARD.

4100 043

JCB

THE MISSION OF AGARD

The mission of AGARD is to bring together the leading personalities of the NATO nations in the fields of science and technology relating to aerospace for the following purposes:

- Exchanging of scientific and technical information;
- Continuously stimulating advances in the aerospace sciences relevant to strengthening the common defence posture;
- Improving the co-operation among member nations in aerospace research and development;
- Providing scientific and technical advice and assistance to the North Atlantic Military Committee in the field of aerospace research and development;
- Rendering scientific and technical assistance, as requested, to other NATO bodies and to member nations in connection with research and development problems in the aerospace field;
- Providing assistance to member nations for the purpose of increasing their scientific and technical potential;
- Recommending effective ways for the member nations to use their research and development capabilities for the common benefit of the NATO community.

The highest authority within AGARD is the National Delegates Board consisting of officially appointed senior representatives from each member nation. The mission of AGARD is carried out through the Panels which are composed of experts appointed by the National Delegates, the Consultant and Exchange Programme and the Aerospace Applications Studies Programme. The results of AGARD work are reported to the member nations and the NATO Authorities through the AGARD series of publications of which this is one.

Participation in AGARD activities is by invitation only and is normally limited to citizens of the NATO nations.

The content of this publication has been reproduced directly from material supplied by AGARD or the authors.

Published July 1979

Copyright © AGARD 1979
All Rights Reserved

ISBN 92-835-1329-0



*Printed by Technical Editing and Reproduction Ltd
Harford House, 7-9 Charlotte St, London, W1P 1HD*

CONTENTS

	Page
ABSTRACT	1
INTRODUCTION	1
CURRENT STATUS	1
HIGH-RELIABILITY APPROACHES	2
SOFTWARE IMPLICATIONS	3
LIGHTNING CONSIDERATIONS	4
FAILURE DETECTION METHODS	4
FUTURE TRENDS	6
CONCLUDING REMARKS	7
REFERENCES	7

Accession For	
NTIS GRA&I	<input checked="checked" type="checkbox"/>
DDC TAB	<input type="checkbox"/>
Unannounced	
Justification	
By _____	
Distribution/	
Availability Codes	
Dist	Avail and/or special
A	

INTEGRITY IN ELECTRONIC FLIGHT CONTROL SYSTEMS

P. R. KURZHALS and R. ONKEN

ABSTRACT

With the increased use of electronic flight-control systems for better aircraft performance and cost-effectiveness, development and test techniques which can insure the integrity of such systems have become critically important. Rapid advances in solid-state electronics have permitted a hundred-fold decrease in control computer size, power and cost over the past two decades. Designers have capitalized on these gains primarily by incorporating additional control functions to improve aircraft capabilities. Resulting control systems have become very complex and reliability requirements have mushroomed. This paper summarizes the evolution of these requirements, outlines the current status of flight control reliability, and highlights promising methods of achieving integrity in future flight control systems.

INTRODUCTION

While reliable control of the flight path has been man's primary concern since the conception of the airplane, modern flight control really came into its own with the automatic flight control systems introduced after World War II. With the advent of the jet engine and the attendant extension of the flight envelope and airplane configuration, designers increasingly turned to the control engineer for help in the solution of the multitude of problems brought on by this new phase of flight.¹

Beginning with the early all-electric autopilots and the first demonstration of automatic flight, resultant control advances, led by electronic technology gains, have revolutionized flight control functions and mechanizations over the past three decades. Replacement of mechanical linkages by computer modules, and the subsequent miniaturization of these modules, have provided the potential for control systems volume and weight reductions of nearly two orders of magnitude. Figure 1 shows the impact of these electronic advances for a representative autopilot subassembly.² A typical 1958 subsystem with about 950 cubic centimeters of circuit cards could - in 1968 - be produced as two microelectronic modules having a volume of less than 50 cubic centimeters. By 1973, hybrid design concepts reduced the volume of these modules to less than 10 cubic centimeters. In practice, much of this potential has been used to add new flight control system functions aimed at further improving aircraft performance.

As a result, flight control applications have evolved from simple pilot-relief autopilots to flight-critical and redundant fly-by-wire and active control systems. To assure the integrity of these systems, more hardware had to be added to achieve the reliability needed for flight safety. Figure 2 illustrated this evolution in complexity.² Early added control system functions, such as command augmentation, could be accommodated with a single, non-redundant channel. As new functions were adopted and the pilot became more dependent on these functions, in-line monitors were included to check the system integrity. For flight-critical implementations which required accommodation of inflight failures, additional levels of redundancy were incorporated to provide fail-safe and fail-operative performance. Redundancy management electronics which provided the circuitry for accuracy enhancement, fault isolation, fault reporting and built-in test rapidly became the dominant part of the system. The related growth in complexity has led to a twenty-fold increase in the number of system elements. Flight control system reliability requirements have increased at an even faster pace and are now comparable to those for the primary structure. As represented in Figure 3 by the probability of computer systems failure for a 10 hour flight period, this increase spans some six orders of magnitude over the past 20 years. Failure probabilities of less than 10^{-9} per flight hour, projected for the flight-critical control systems of the next generation of aircraft, thus present a major and relatively unexplored challenge to the flight control system designer.

CURRENT STATUS

The current status of flight control systems reliability can best be assessed by reviewing the performance of state-of-the-art avionics hardware through the analysis of a quantifiable parameter such as MTBF (Mean Time Between Failures). One such study³ assessed some 98 different types of avionics equipment. Over 1.2 million aircraft failures observed during more than a million flight hours were included in the analysis. Avionics subsystems were found to be involved in more aircraft failures than any other aircraft subsystem, with the proportion of avionics failures to total failures ranging from 27% for helicopters to 52% for supersonic fighters. Avionics subsystems were found to experience one failure every 2.8 flight hours, on average. As shown in Figure 4, only 45% of the failures studied were traceable to specific hardware and software causes. The remaining 55% were classified either as hardware failures with unknown causes (26%) or as an anomaly (29%), defined as any failure which could not be verified in maintenance checkout. For equipment procured under contracts which included an MTBF specification as part of the over-all design criteria, less than 25% of the specified MTBF was actually achieved in the field. Even so,

MTBF's were higher by a factor of 1.4 in equipment procured under contracts containing an MTBF specification than in equipment procured with no MTBF specification.

The difficulties in achieving specified reliability standards, and in diagnosing failures in modern avionics equipment, underscore the need for reliable design concepts and methods for future aircraft flight control systems.

HIGH-RELIABILITY APPROACHES

High-integrity flight control systems must achieve required reliability standards while maintaining an appropriate balance among the competing factors of cost, scheduling, and performance. Thus, reliability should be an inherent element of the total design approach, with responsibility for attaining established reliability goals assigned (and accepted) early in the conceptual stages of design. By addressing the question of high system reliability throughout the design process, many resources (both dollars and hours) can be saved which would otherwise have to be devoted to after-the-fact design alterations. The fail-and-fix approach to system reliability, inherently inefficient in general, is particularly ineffective in eliminating those design problems which result in relatively infrequent failures. This is especially relevant for future complex avionics and flight control mechanizations, which are characterized by thousands of potential failure modes, none of which may repeat often enough to assure their elimination.

Considerable design and test experience for such analog⁴ and digital^{5,6} fly-by-wire flight control systems has been obtained. Figure 5 illustrates a representative advanced flight control system, the digital fly-by-wire system developed and tested by NASA on an F-8 aircraft. Typical elements of such a system include sensor modules to determine the aircraft state and errors from a desired path, processing electronics and networks to generate the necessary control commands, and actuators to drive the aircraft control surfaces. Reliability characteristics for each of these elements and for the total system must be considered to assure adequate flight control integrity.

Sensors

Accelerometers, gyros, and differential transformers are the most commonly used sensors in automatic flight-control systems. Since servonulled linear accelerometers and linear variable differential transformers have well-established records for reliability and are likely to continue to be used in highly-reliable flight control applications in the future, the greatest improvements in sensor reliability will probably be made in angular rate sensors. Spin motor and bearing failures account for most rate gyro failures; it is therefore likely that future highly reliable control systems will feature angular rate sensors which do not employ these components. Ring laser gyros and magnetohydrodynamic rate sensors are currently being designed to alleviate this problem. These sensors achieve high reliability by minimizing many of the wearout modes caused by moving mechanical parts.

Higher reliability can also be achieved by applying skewed sensor techniques to reduce the number of rate gyros required in a given flight control system. In addition to increasing reliability by reducing the number of parts which can fail, the skewed sensor approach results in savings of weight, power, and volume.⁷

Another approach uses analytic redundancy instead of redundant sensor hardware. This is accomplished by exploiting the knowledge about the aircraft dynamics and coupling of the aircraft state-vector components for the implementation of observer filters which provide additional information about the aircraft state. By use of the observer signals, failure detection and voting can be easily achieved and the number of sensor devices can be reduced without reducing reliability.⁸

Electronics

Potential reliability problems caused by defective electronic components can be minimized by incorporating component redundancy into the design process. Some drawbacks to the component redundancy method should be borne in mind, however. The most obvious difficulties are due to the increase in parts count inherent in this approach. Additional parts result in increased size, weight, cost, power consumption and power losses, all of which add undesirable and sometimes unnecessary complications to the total design process. Furthermore, successful exploitation of the component-redundancy approach requires a certain amount of a priori information about the failure mechanism which is to be eliminated. For example, one would probably apply a parallel arrangement of redundant components if the most likely failure were an open circuit, while short circuits are better accounted for by arranging components in series. A relatively complex arrangement of redundant components is required to protect against all possible combinations of component failures. Figure 6 illustrates the problem facing the designer when he uses redundancy to protect against component failures in even a simple application. Reliable information about probable failure modes is difficult enough to obtain after a failure has occurred; it is that much more difficult to generate such information in an a priori fashion during the design stage.

The problems associated with defining a priori the most likely component failure modes can be eliminated by applying the redundancy method on a system level in which any failure in a prime system results automatically in a shut-down of the prime system and a simultaneous switch to the first of one or more back-up systems. Subsystem redundancy entails the same fundamental restrictions as component redundancy (increased size, weight, cost) but, as discussed earlier, leads to an enormous increase in system complexity

and sophistication. In addition to providing in the backup system or systems all the functional capabilities of the prime system, it is also necessary to incorporate some means for detecting prime system failures in real-time and for switching from prime to back-up systems. Currently research is being sponsored at several places to develop the technology of fault-tolerant computer systems for application where extremely high reliability is required, with both hardware and software methods being investigated.^{9,10} The fault-tolerant computer used in future flight-control applications will be capable of detecting computer-system errors. It will further be able to assess the error and take corrective action as appropriate. For example, the highly-reliable computer will be capable of altering its internal processing procedures through reconfiguration to bypass the fault which has been detected. The application of such fault-tolerant techniques will eventually allow the power of real-time computer processing to be applied even in flight-critical applications.

Actuators

Hydraulic actuators are used extensively in highly reliable flight-control systems and reliability is achieved through the application of advanced technology at both the component and the system level. On the component level, improvements which continue to be made in hydraulic fluids, tube connectors, tube materials, seals, and filtration techniques will ultimately result in enhanced reliability for the entire flight control system. New system-level technology under consideration includes high-pressure fluid-distribution systems to achieve substantial reductions in space and weight with improved maintainability and reliability. Integrated actuators, capable of positioning the control surface directly from an electrical command, will likely be a part of future highly reliable control systems.

Reliability in actuator systems is often achieved by the application of various redundancy methods. The multicylinder hydraulic actuator is in widespread use and is found in a large number of configurations. Dual and triple designs of tandem cylinders have been built, as have multiple single cylinders, to achieve enhanced reliability. Combinations of independent control surfaces operated by individual actuators are also used to further improve control system reliability.¹¹ For the purpose of enhanced failure detection in redundant actuators, digital or incremental technology can be applied to the electro-hydraulic part of such systems.^{12,13}

SOFTWARE IMPLICATIONS

The importance of software reliability is often underestimated when the question of overall system reliability is considered. It is assumed that software errors are found during debugging and testing and that the probability that a hardware component or subsystem will fail represents the essence of the system reliability concept. Unfortunately, errors in the assembly of software code are as likely to escape "final check-out" as the design and fabrication shortcomings which eventually lead to hardware failures.

Figure 7 indicates the evolution of computer hardware and software costs. Note that the ratio of software costs to total system costs is growing rapidly. This reflects in part recent and projected decreases in the cost of computer hardware, but the trend is also due to the growing size and complexity of modern software operating systems. It is to be expected that this increase in software sophistication will be accompanied by a corresponding increase in systems-reliability problems associated with software errors.

The relative importance of software reliability becomes clearer when one realizes that, in current electronic flight control systems, software costs exceed computer hardware costs by a factor of three to four and that the largest effort in developing software is due to the testing, correction, retesting, release, recall, correction, and re-release of software.¹⁴ The task of developing the original code is quite small in comparison. Figure 8 represents the estimated and actual costs of developing software for a representative system.¹⁵ This figure illustrates that software costs are often unanticipated, or at best underestimated, and that considerable effort is routinely expended in the post-production stage of system development to correct software-related errors.

The magnitude of this problem can be further appreciated when one realizes that, while the hardware designer has at his disposal a wide range of design methodologies and alternatives to use in optimizing hardware reliability, the software designer does not. Historically his objective has been limited to developing coding to the point that it "works"; that is, to the point that the software program consistently produces expected results from a set of known inputs.

When the concept of hardware reliability was originally conceived, hardware-systems engineering was a well-developed field. By contrast, the problem facing software designers is that coding is fundamentally an art form, with no generalized methodology available for guidance in the development of software.

Structured programming techniques¹⁶ and standardized higher-order languages¹⁷ do offer some promise of segmenting and simplifying future software generation. Compiler writing systems, first developed by DOD and now being extended by NASA, can further aid this process by automatically translating programs written in a higher order language into machine language for a candidate flight computer. Used with software-reference libraries, which assemble commonly-used software algorithms such as quadratic filters, and with built-in validation and verification programs, these compiler writing systems can significantly decrease the cost of the many iterations and changes inherent in the design of flight control systems.

Other software reliability-assurance systems,¹⁸ under development by NASA, will be capable of detecting and assessing errors and reconfiguring the operating systems in such a way that the error mechanism which has been detected is by-passed. In a parallel effort, a number of reliability assessment methods are being designed to provide the design engineer with a yardstick for measuring the reliability of complex computer systems. An example of such an effort is the computer-aided reliability analysis (CARE) program developed by the Langley Research Center.¹⁹ This program calculates the reliability of a given fault-tolerant system model and is currently being extended to include multiply-redundant, highly-reliable computer configurations.

While efforts are under way within NASA, as well as in industry and DOD, to develop a consistent software design methodology,²⁰ progress in this extremely difficult and complex endeavor is necessarily slow. With the rapid advances now being witnessed in the technology of reliable, solid-state hardware, it is becoming increasingly likely that future systems reliability will be paced more and more by developments in software engineering or that much future software will be replaced by hard-wired equivalents or firmware.

LIGHTNING CONSIDERATIONS

Flight control systems must operate in an environment in which severe electrical transients caused by lightning strikes are likely, if not certain, to occur. Lightning strikes on representative transport aircraft have occurred about once per 2500 flight hours.²¹ It is important that the designer understand the lightning threat and allow for it in the design of avionics and flight control systems.

As illustrated in Figure 9, a typical lightning flash always involves an entry point and an exit point on the aircraft.²² Usually these points are extremities on the aircraft, such as the nose and wing tip. Each lightning flash is composed of a number of high current strokes, with peak currents ranging from 30,000 amperes for a moderate stroke to around 200,000 amperes for a severe stroke. The total lightning event may last from 0.1 to 1 second, with continuous currents on the order of several hundred amperes between strokes.

Lightning current flowing through the structural resistance of the aircraft produces a voltage which can be thought of loosely as an IR drop across the structure. Circuits with multiple connections to the aircraft structure will have this voltage developed across the corresponding terminals. Such IR effects can be countered by employing a single point ground to the aircraft frame or by using differential wiring in which wires are provided for signal and power return paths instead of the aircraft frame.

Some insight into the severity of the lightning problem can be gained by reviewing the results of electrical transient tests conducted in 1973 on the NASA F-8 Digital Fly-by-Wire (DFBW) aircraft.²²

In these tests, simulated lightning strikes at a non-destructive level of 300 amperes were applied to an early configuration of the DFBW aircraft while voltage and current measurements were made in various circuits. Results of measurements at this level were then scaled up by assuming a lightning current of 30,000 amperes. Voltages (for a 30,000 ampere strike) in the range of 60 to 120 volts were determined in the Apollo guidance computer with levels on the order of 200 volts for the power busses. Currents measured in the wire bundles located in the left gun bay indicated that up to 180 amperes peak-to-peak would be induced by a 30,000 ampere strike. Figure 10 illustrates the resultant distribution of current amplitudes in the cable bundles. These levels, if not protected against, would exceed the typical 10 ampere peak current specified for electronic flight control systems.

The designer basically has two options for incorporating lightning resistance into his design. He can attempt to insure that all sensitive circuits are contained within a transient-free environment or he can specifically design the system to accept transients at all terminals.

The first approach usually employs a Faraday-Cage grounded chassis construction, with the input power carefully filtered and all wires connecting to other subsystems thoroughly shielded. The details of the second approach depend on the specifics of the system being designed, but certain general practices include coupling transformers to protect sensitive circuits from common-mode surges, balanced transmission lines and grounded shields on all transmission cables, and voltage clamps on signal leads.

FAILURE DETECTION METHODS

Failure detection is one of the keys to high system reliability. Generally, failures are detected at the component level prior to fabrication, or at the system level after fabrication. Both failure detection methods will be considered briefly in this section.

Component Failures

Since the cost of detecting faults on the component level is 1/3 the cost of detecting failures at the system level,²³ the importance of component failure detection cannot be overemphasized. The purpose of component testing is of course, to screen out faulty components in the beginning and to gain some insight as to how the performance of a good

component will vary over its lifetime as it is exposed to its operational environment in a specific user task. As shown in Figure 11, the probability of failure decreases with time during the initial or "burn-in" phase of the components life-time, reaching a minimum constant level.²⁴ After some period of time, the probability of failure begins to increase with time, reflecting the influence of wear-out failures. The essence of component testing is to try to predict the parameters of this curve for the component under evaluation.

Component testing methods can be classified as either destructive or non-destructive. Each category includes environmental, physical, and electrical tests. Examples of destructive environmental tests are operation of the component to failure under extremes of humidity or pressure, or through exposure to salt spray or corrosive solvents. In destructive physical tests, components are inspected after being subjected to radial, axial, and tension forces, and twisting or bending moments. Destructive electrical tests include tests for voltage breakdown in dielectrics and insulators, and tests for input protection in electronic components susceptible to damage from static discharge, such as MOS integrated circuits.

There are a very wide range of non-destructive environmental tests including thermal tests which measure component performance at constant temperature and in large thermal gradients, and mechanical tests in which component performance is measured in the presence of vibration, acceleration, and mechanical shock.

Non destructive physical tests include leak tests for hermiticity and x-ray tests to detect loose foreign particles within a component assembly. Non-destructive electrical tests are many and varied and the details of the test depend on the component to be tested. In general, nondestructive electrical component tests are designed to determine whether the component performs a specified function as the result of a given input. Examples include tests to determine if resistance and capacitance values are within specified tolerance ranges and state tests on integrated circuit logic gates.

System Failures

The failure detection at the system level is most important, as it determines the efficiency of the redundancy concept used in the system. Two basic modes of failure detection have to be considered together, the off-line detection (pre-flight-test) and the on-line detection during system operation (built-in test). Both have to be coordinated very carefully, because the thoroughness of the total detection effort determines, whether the failure probability increases from mission to mission or whether the probability can be assumed to start for each mission at the same level.

It is possible to improve system reliability and at the same time reduce support costs and turn-around time by including built-in test (BIT) capability in the design of digital flight control systems. Figure 12 illustrates the potential impact of BIT on system reliability.

There are a great number of hardware and software techniques and methods for on-line failure detection at the designer's disposal. In order to be able to judge their efficiency and their effect on the system integrity the essential principles of failure detection are briefly described. Failure detection in real system designs can use all possible combinations of these principles.

The fundamental detection principle which must be applied in all cases is the comparison of signals which result from functionally equivalent processing units. These signals are independently derived from the same input signal and are usually dependent on the status of the process. Discrepancies at the comparator indicate a malfunction. The other basic principle is the test principle. The objective of the test method is to ensure that the input signal adequately exercises all components in the system. The way of applying the test principal determines how long it takes for a malfunction to become evident. The higher the test frequency for all processing states, the faster is the detection of any malfunction. There are two basic approaches to applying the test principle. One is independent of the process and its status and the other is dependent on the status of the process. In the latter case, the test signal is simply the unmodified input signal on which the system is working, determined by the process and its statistics and not provided by any specific detection device. This is defined as passive failure detection, as opposed to active failure detection, where the input signal is derived independently for the purpose of a complete component test. In the active case, there are periodical tests of all states of each system component. For some methods of active failure detection the test is carried out simultaneously with the system process; otherwise process interrupts are necessary for this kind of testing. It is of great importance for the overall integrity, that the failure detector or voter can diagnose its own failures, too. This can easily be achieved, when active failure detection is used.¹³

The evaluation of the design of flight control systems with respect to the integrity (i.e. the redundancy and failure detection concept, subject to mission efficiency and cost) is very difficult because of the great variety of possible approaches and the complexity of the system. Related investigations include a comparison between the usual passive failure detection methods with comparison testing of redundant systems and pure active failure detection with very high test frequency.⁸ The probability of total loss based on failure detection information, which is attainable during the system operation, was used as an criterion instead of the number of failures to be survived. Some of the more commonly used test techniques are briefly outlined here. As far as the sensors are concerned, only passive failure detection is possible, because the sensor inputs cannot

be influenced by the control system. That means, comparison testing of the output signals of redundant sensor units is necessary.

Where the degree of redundancy is not sufficient to permit voting, the designer may employ various real-time modeling techniques, as already mentioned earlier. These techniques may also use the fact that outputs from independent sensors are compared. For example, the output of an accelerometer displaced from the aircraft center of gravity may be used to check the output of a rate gyro.

For systems in which signals may be present in a given element for only short periods of time, separated by long, quiescent periods, active failure detection can be readily applied. The self-testing can be accomplished through stimulated monitoring. In stimulated monitoring, a small tracer signal, generally with zero mean value, is passed through the system and the output. The stimulus is always selected to have negligible effect on system performance.

One of the simplest self-testing methods available is the fixed-model method, in which comparisons are made to ensure that the control system's signals or certain carrier characteristics (i.e. pulse frequency and shaping) agree with expected ones within prescribed limits for a given set of conditions. This method can be implemented either in hardware or in software. Examples include parity checks and memory-sum checks. These methods can be either passive or active.

For systems involving communication with one or more asynchronous peripherals, the "handshake" method is often used. Handshake communication methods require that the receiver generates a "ready" signal before the sender will pass signals. Received signals are then compared with transmitted signals to insure that they are identical. If they are not, additional transmission may be attempted, until there is a match.

Processor timing can be used in a very simple self-test method to test for software errors. In a properly functioning program a clock within the processor is reset at regular intervals. An early or late reset is interpreted as evidence of some difficulty.

For digital control systems with a finite and known set of digital output patterns, self-test circuits can be used to detect errors. An error signal is generated whenever the output differs from the known set of "good" code words.

We have briefly touched on a few of the more common self-testing methods applicable to flight control systems which the designer has at his disposal. Constraints imposed by the details of the system being designed dictate to a great extent which self-test method, if any, makes the most sense. Clearly, self-testing, when used in conjunction with other methods outlined in this paper, has the potential for sharply increasing the reliability of flight control systems.

FUTURE TRENDS

The number of flight-critical functions, such as automatic landing and active control, now performed by modern flight control systems are expected to continue to increase in the future. As we move into the era of integrated control, flight control is rapidly becoming an equal partner with aerodynamics, propulsion and structures in the aircraft design process.²⁵ This integrated view of airframe, propulsion and subsystem control functions and mechanizations, illustrated in Figure 13, will be a principal driver in the efficiency and economics of future aircraft. Major improvements in aircraft performance and reductions in aircraft weight appear possible through combinations of currently-independent aircraft functions such as active airframe control, propulsion control, landing loads control, and fuel management. For example, the integration of active landing gear and maneuver load control systems can appreciably decrease wing structural stiffness requirements and weight. Similarly, automatic reconfiguration of control system gains in the event of an engine failure can allow sizeable reductions in required control surface areas. Extensions of this approach to fully-integrated, control-configured aircraft could provide up to 15% fuel savings and structural weight reductions.

In addition, integrated control will permit the evolution of a distributed control architecture which utilizes a redundant data bus and standard microprocessor modules to implement all aircraft control functions. Such standard programmable modules would have built-in fault tolerance, multifunctional capability, and standard interfaces to yield significantly fewer control system elements and lower system costs.²⁶ For example, application of this design approach to a B-737 transport could reduce the number of standard boxes from the 64 now used to 20 standard modules with attendant weight savings of about 1000 lbs. Potential gains in reliability could be even more important. Preliminary analyses indicate that integrated control configurations could be implemented with twice the reliability, half the maintenance cost, and one-third the equipment used in present flight control systems. Projected component advances will further increase flight control system performance and integrity. Examples of these include solid-state or ring laser rate gyros, very high-density integrated circuits and multi-layered packaging techniques, fiber optics data links with their inherent potential for lightning survivability, and light-weight electrohydraulic actuators. With the flexibility afforded by digital electronics and fly-by-wire systems, future flight control design could be significantly simplified and specific systems could be readily mechanized through the assembly of proven sensor, processor, and actuator modules using the latest technology.²⁷

CONCLUDING REMARKS

Flight control systems today stand at the threshold of a new age - in terms of both utilization and mechanization. The first steps, fly-by-wire and active control, have already been taken in operational military aircraft and are being designed into the civil transports now on the drawing boards. Beyond that, the revolution in microelectronics and related technologies offers the promise of totally-integrated control functions and simplified system configurations which take maximum advantage of standardized modules to increase reliability while reducing systems development and maintenance costs.

The integrity of flight control has been, and will continue to be, the key factor in the acceptance of these concepts for operational application. While considerable progress has been made in this area, major additional gains in reliable design approaches and implementations are essential if flight control systems are to reap their full benefits during the next decade.

REFERENCES

1. McRuer D.: "A Historical Perspective for Advances in Flight Control Systems." AGARDograph AG-224, May 1977
2. Osder, S.S.: "Chronological Overview of Past Avionic Flight Control System Reliability in Military and Commercial Operations." AGARDograph AG-224, May 1977
3. Bird, G.T. and Hird, G.R.: "Experienced Inflight Avionics Malfunctions." AGARD LS-81, April 1976
4. Ramage, James K. and Morris, James W.: "Design Considerations for Reliable Fly-By-Wire Control." Paper presented at the AGARD Symposium on Stability and Control, Ottawa, Canada, September 1978
5. Szalai, K.J. et.al.: "Design and Test Experience with a Triply Redundant Digital Fly-By-Wire Control System." AGARDograph AG-224, May 1977
6. Robinson, P.; Meadows, I.; and Copage C.M.: "A High Reliability, High-Integrity Flight Control System." AGARDograph AG-224, May 1977
7. Potter, J. and Suman, M.: "Thresholdless Redundancy Management with Arrays of Skewed Instruments." AGARDograph AG-224, May 1977
8. Task-Oriented Flight Control System. AGARD - LS-89, 1977
9. Murray, N.D.; Hopkins, A.L.; and Wensley, J.H.: "Highly Reliable Multi-processors." AGARDograph AG-224, May 1977
10. Onken, R.: "System Integrity by Use of Selfdiagnosing Failure Detection." AGARDograph AG-224, May 1977
11. Early, B.: "Objectives for the Design of Improved Actuation Systems." AGARDograph AG-224, May 1977
12. Post, K.H.: "Study of Electrohydraulic Control Valves with Fluidic Ball Elements." ESRO TT-112, 1974
13. Doetsch, K.H.: "The proper Symbiosis of the Human Pilot and Automatic Control System." Aeronautical Journal, 1975
14. Shooman, M.L.: "Software Reliability: Analysis and Prediction." AGARDograph AG-224, May 1977
15. Sokol, Q.M.: "Centrally-Designed Data Systems." 1975
16. Mills, H.D.: "Structured Programming." Proceedings of Fault-Tolerant Systems Workshop, Research Triangle Institute, January 1976
17. Belcher, G. and Egan T.: "Software Integrity through Visibility." AGARDograph AG-224, May 1977
18. Conn, R.B.; Merryman, P.M.; and Whitelaw, K.L.: "CAST: A Complementary Analytic-Simulative Technique for Modeling Complex, Fault-Tolerant Computing Systems." AGARDograph AG-224, May 1977
19. Raytheon Co.: "An Engineering Treatise on the CARE-II Dual Mode and Coverage Models." NASA CR-144993. April 1976
20. AIAA Professional Seminars: "Software Management: Define Systems and Other Federal Program, Parts I and II." 1976/1977
21. Bjurman, B.E. et.al.: "Airborne Advanced Reconfigurable Computer System." NASA CR-145024, August 1976

22. Fisher, F.A.: "Lightning Considerations on the NASA F-8 Phase II Digital Fly-By-Wire System." General Electric SRD-75-074, June 1975
23. GSFC Quality Assurance Brief. QAB No. 72-10, October 1972
24. Schambeck, W.: "Reliability Testing of Electronic Parts." AGARD-LS-81, April 1976
25. Proceedings of AGARD-Conference on "Impact of Active Controls on Airplane Designs." AGARD CP-157, 1975
26. A Study of Standardization Methods for Digital Guidance and Control Systems. AGARD, AR-90
27. Arnold, James I.: "Future Trends in Highly Reliable Systems, AGARDograph AG-224, May 1977

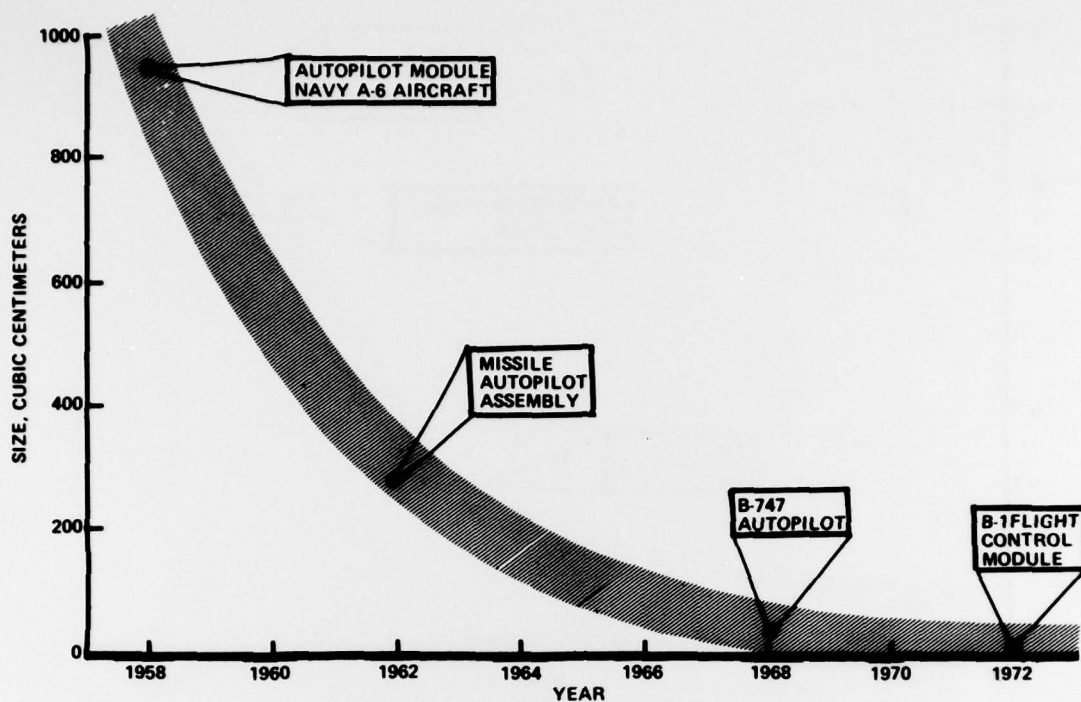


Fig.1 Miniaturization of representative flight control hardware

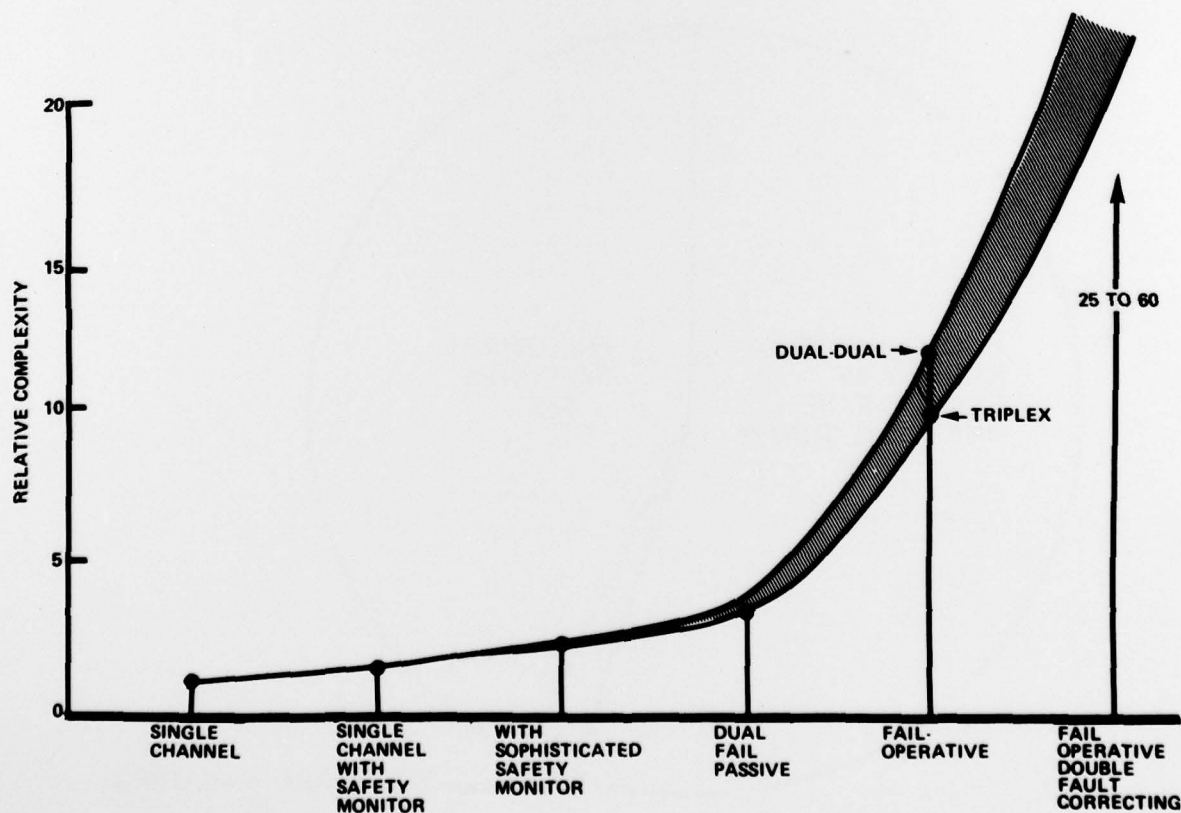


Fig.2 Effect of redundancy on control complexity

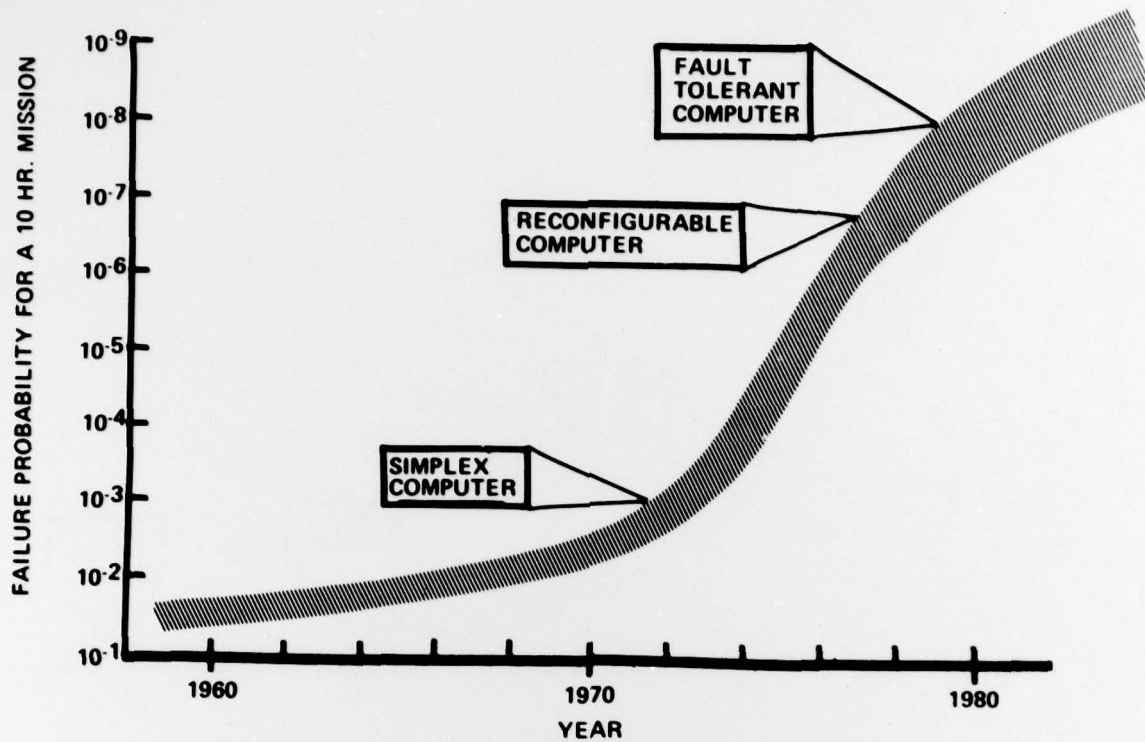


Fig.3 Computer system reliability

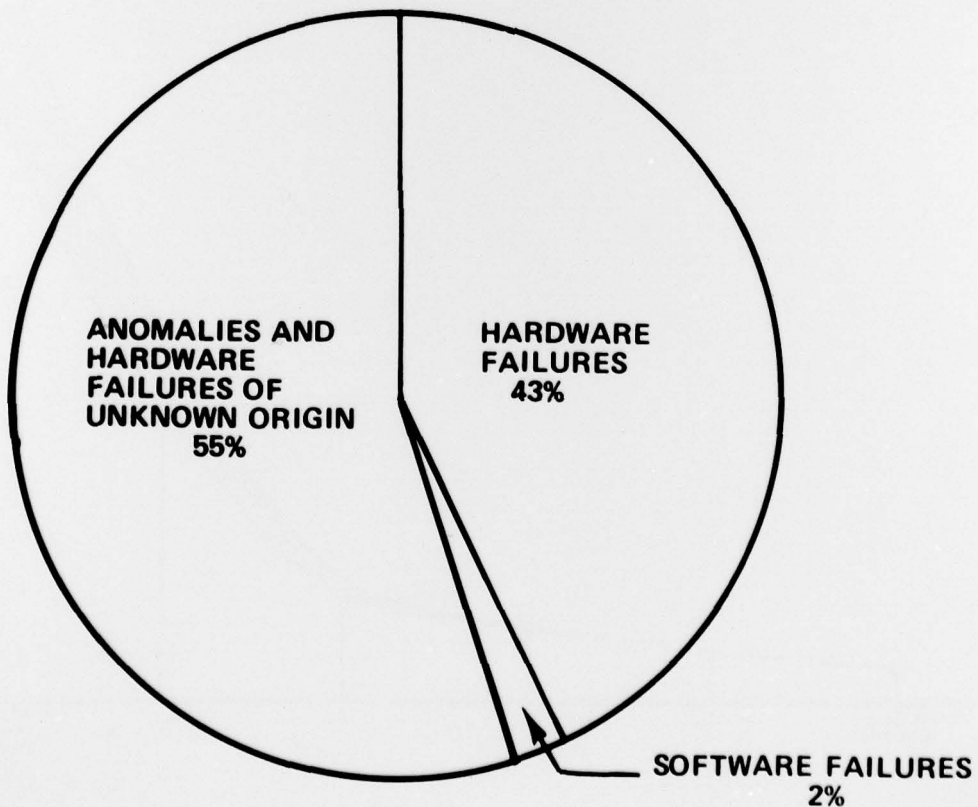


Fig.4 Distribution of avionics failures

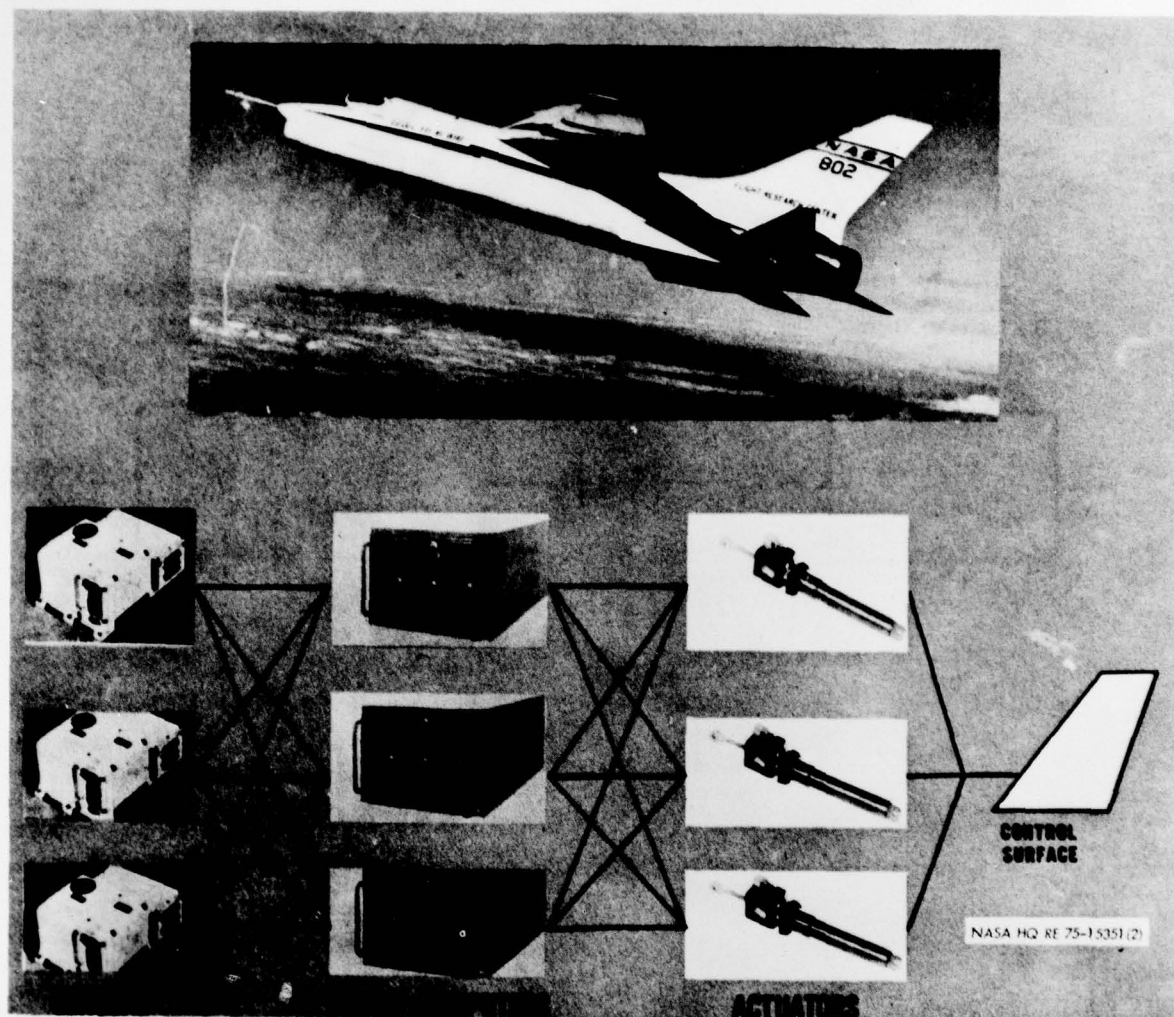


Fig.5 Typical flight control system

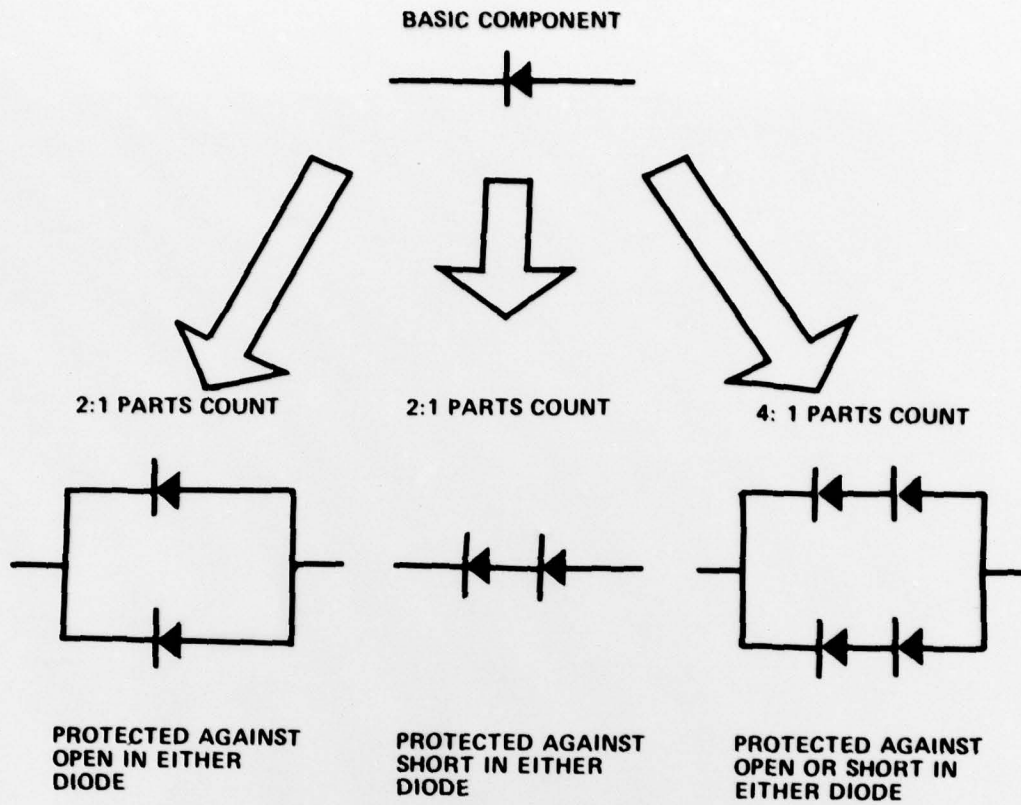


Fig.6 Representative redundancy configurations for component failure protection

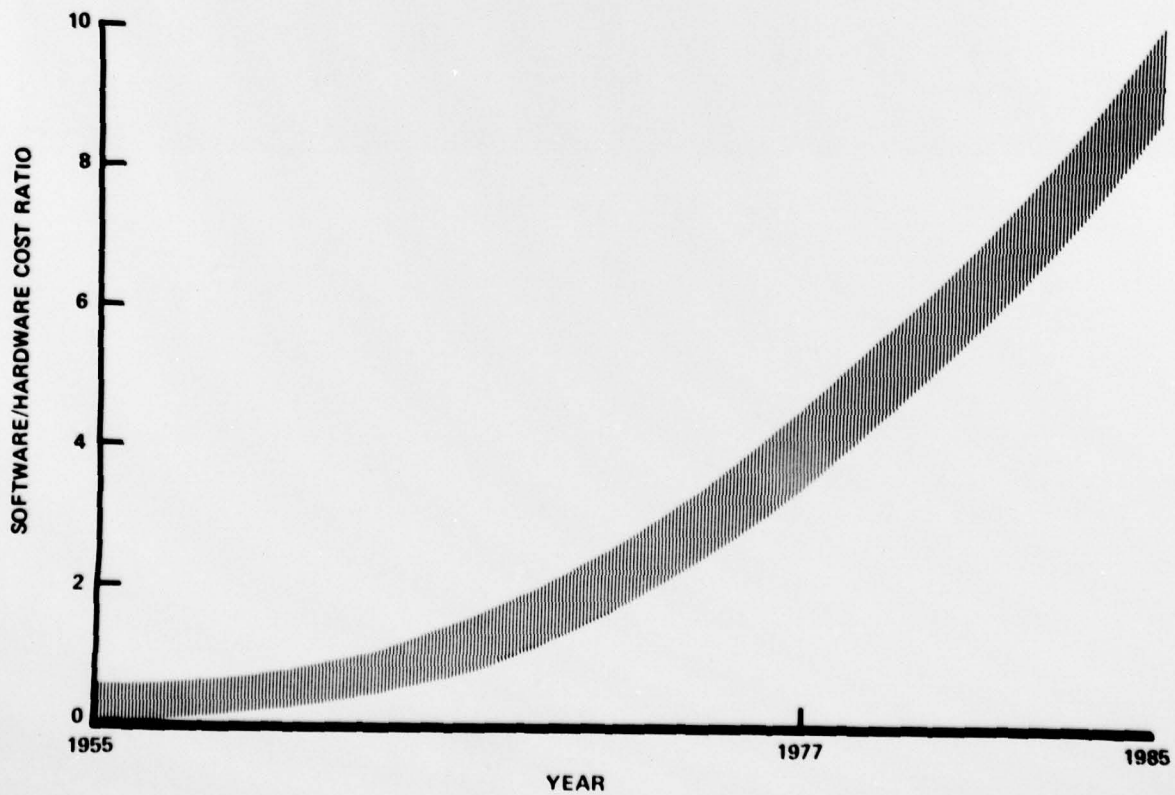


Fig.7 Hardware/software cost relationship

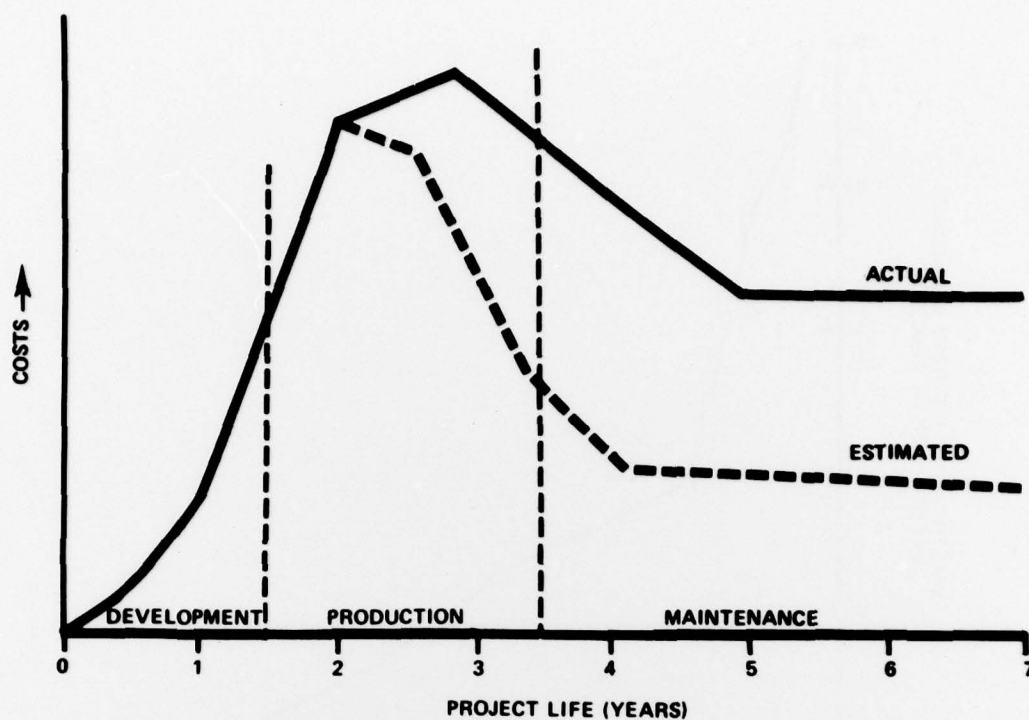


Fig.8 Computer system budget cycle

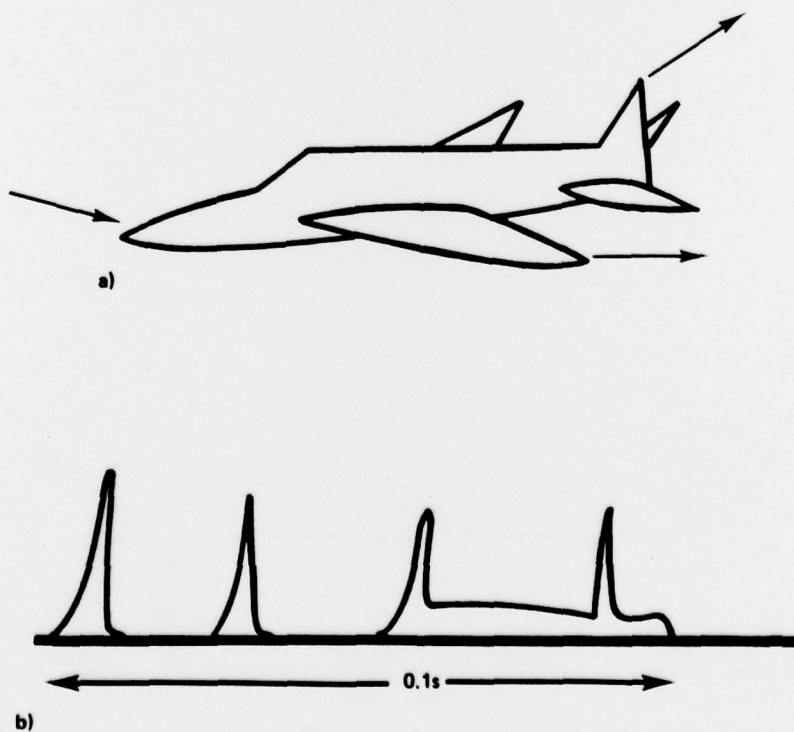


Fig.9 The lightning environment
 (a) Entry and exit points
 (b) Typical flash composed of discrete strokes

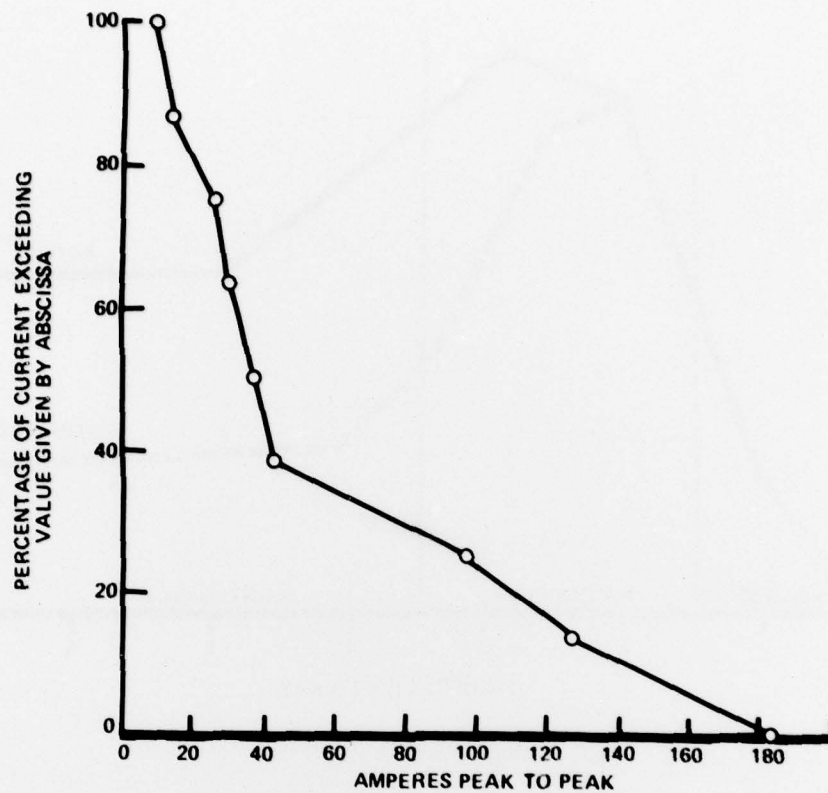


Fig.10 Distribution of current amplitudes in cable bundle for 30,000 ampere lightning strike

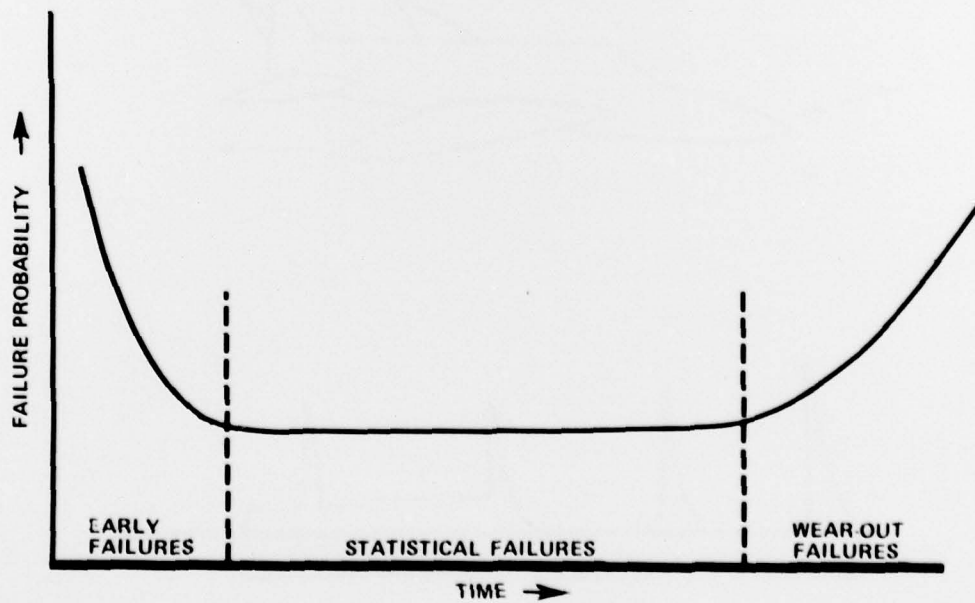


Fig.11 Circuit failures vs time

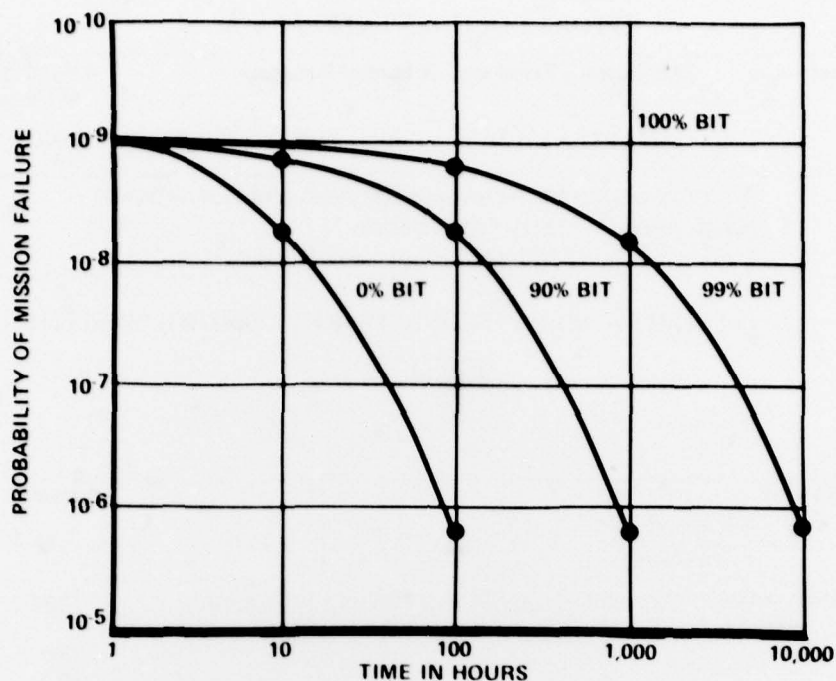


Fig.12 Effect of bit testing on probability of mission failure



CONTROL SYSTEM DEVELOPMENT

DISTRIBUTED
ARCHITECTURE

STANDARD
MODULES

MULTIFUNCTIONAL
USAGE

BUILT-IN FAULT
TOLERANCE

FEWER SYSTEM ELEMENTS
LOWER SYSTEM COSTS

A/C APPLICATION

ACTIVE AIRFRAME CONTROL

+

ACTIVE PROPULSION CONTROL

+

ACTIVE LANDING LOADS CONTROL

+

ACTIVE FUEL MANAGEMENT

+

.....

REDUCED A/C WEIGHT
INCREASED A/C EFFICIENCY

Fig.13 Integrated control concepts

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's Reference	3. Further Reference	4. Security Classification of Document								
	AGARD-AR-136	ISBN 92-835-1329-0	UNCLASSIFIED								
5. Originator	Advisory Group for Aerospace Research and Development North Atlantic Treaty Organization 7 rue Ancelle, 92200 Neuilly sur Seine, France										
6. Title	INTEGRITY IN ELECTRONIC FLIGHT CONTROL SYSTEMS										
7. Presented at											
8. Author(s)/Editor(s)	P.R.Kurzahls* R.Onken†		9. Date July 1979								
10. Author's/Editor's Address	*Director, Guidance Control and Information Systems Division, National Aeronautics and Space Administration, Washington, DC 20546, USA †DFVLR, Institut für Flugführung, Flughafen, D-3300 Braunschweig		11. Pages 20								
12. Distribution Statement	This document is distributed in accordance with AGARD policies and regulations, which are outlined on the Outside Back Covers of all AGARD publications.										
13. Keywords/Descriptors	<table border="0"> <tr> <td>Flight control</td> <td>Airborne equipment</td> </tr> <tr> <td>Avionics</td> <td>Man-machine systems</td> </tr> <tr> <td>Reliability (electronics)</td> <td>Solid state devices</td> </tr> <tr> <td>Design criteria</td> <td></td> </tr> </table>			Flight control	Airborne equipment	Avionics	Man-machine systems	Reliability (electronics)	Solid state devices	Design criteria	
Flight control	Airborne equipment										
Avionics	Man-machine systems										
Reliability (electronics)	Solid state devices										
Design criteria											
14. Abstract	<p>With the increased use of electronic flight-control systems for better aircraft performance and cost-effectiveness, development and test techniques which can insure the integrity of such systems have become critically important. Rapid advances in solid-state electronics have permitted a hundred-fold decrease in control computer size, power and cost over the past two decades. Designers have capitalized on these gains primarily by incorporating additional control functions to improve aircraft capabilities. Resulting control systems have become very complex and reliability requirements have mushroomed. This paper summarizes the evolution of these requirements, outlines the current status of flight control reliability, and highlights promising methods of achieving integrity in future flight control systems.</p> <p>This Advisory Report was sponsored by the Guidance and Control Panel of AGARD.</p>										

<p>AGARD Advisory Report No. 136 Advisory Group for Aerospace Research and Development, NATO</p> <p>INTEGRITY IN ELECTRONIC FLIGHT CONTROL SYSTEMS</p> <p>by P.R.Kurzahls and R.Onken Published July 1979 20 pages</p> <p>With the increased use of electronic flight-control systems for better aircraft performance and cost-effectiveness, development and test techniques which can insure the integrity of such systems have become critically important. Rapid advances in solid-state electronics have permitted a hundred-fold decrease in control computer size, power and cost over the past two</p> <p>P.T.O.</p>	<p>AGARD-AR-136</p> <p>Flight control Avionics Reliability (electronics) Design criteria Airborne equipment Man-machine systems Solid state devices</p>	<p>AGARD-AR-136</p> <p>Flight control Avionics Reliability (electronics) Design criteria Airborne equipment Man-machine systems Solid state devices</p>	<p>AGARD-AR-136</p> <p>Flight control Avionics Reliability (electronics) Design criteria Airborne equipment Man-machine systems Solid state devices</p>	<p>AGARD-AR-136</p> <p>Flight control Avionics Reliability (electronics) Design criteria Airborne equipment Man-machine systems Solid state devices</p>	<p>AGARD-AR-136</p> <p>Flight control Avionics Reliability (electronics) Design criteria Airborne equipment Man-machine systems Solid state devices</p>
<p>AGARD Advisory Report No. 136 Advisory Group for Aerospace Research and Development, NATO</p> <p>INTEGRITY IN ELECTRONIC FLIGHT CONTROL SYSTEMS</p> <p>by P.R.Kurzahls and R.Onken Published July 1979 20 pages</p> <p>With the increased use of electronic flight-control systems for better aircraft performance and cost-effectiveness, development and test techniques which can insure the integrity of such systems have become critically important. Rapid advances in solid-state electronics have permitted a hundred-fold decrease in control computer size, power and cost over the past two</p> <p>P.T.O.</p>	<p>AGARD-AR-136</p> <p>Flight control Avionics Reliability (electronics) Design criteria Airborne equipment Man-machine systems Solid state devices</p>	<p>AGARD-AR-136</p> <p>Flight control Avionics Reliability (electronics) Design criteria Airborne equipment Man-machine systems Solid state devices</p>	<p>AGARD-AR-136</p> <p>Flight control Avionics Reliability (electronics) Design criteria Airborne equipment Man-machine systems Solid state devices</p>	<p>AGARD-AR-136</p> <p>Flight control Avionics Reliability (electronics) Design criteria Airborne equipment Man-machine systems Solid state devices</p>	<p>AGARD-AR-136</p> <p>Flight control Avionics Reliability (electronics) Design criteria Airborne equipment Man-machine systems Solid state devices</p>

<p>decades. Designers have capitalized on these gains primarily by incorporating additional control functions to improve aircraft capabilities. Resulting control systems have become very complex and reliability requirements have mushroomed. This paper summarizes the evolution of these requirements, outlines the current status of flight control reliability, and highlights promising methods of achieving integrity in future flight control systems.</p> <p>This Advisory Report was sponsored by the Guidance and Control Panel of AGARD.</p>	<p>decades. Designers have capitalized on these gains primarily by incorporating additional control functions to improve aircraft capabilities. Resulting control systems have become very complex and reliability requirements have mushroomed. This paper summarizes the evolution of these requirements, outlines the current status of flight control reliability, and highlights promising methods of achieving integrity in future flight control systems.</p> <p>This Advisory Report was sponsored by the Guidance and Control Panel of AGARD.</p>
<p>ISBN 92-835-1329-0</p>	<p>ISBN 92-835-1329-0</p>
<p>decades. Designers have capitalized on these gains primarily by incorporating additional control functions to improve aircraft capabilities. Resulting control systems have become very complex and reliability requirements have mushroomed. This paper summarizes the evolution of these requirements, outlines the current status of flight control reliability, and highlights promising methods of achieving integrity in future flight control systems.</p> <p>This Advisory Report was sponsored by the Guidance and Control Panel of AGARD.</p>	<p>decades. Designers have capitalized on these gains primarily by incorporating additional control functions to improve aircraft capabilities. Resulting control systems have become very complex and reliability requirements have mushroomed. This paper summarizes the evolution of these requirements, outlines the current status of flight control reliability, and highlights promising methods of achieving integrity in future flight control systems.</p> <p>This Advisory Report was sponsored by the Guidance and Control Panel of AGARD.</p>
<p>ISBN 92-835-1329-0</p>	<p>ISBN 92-835-1329-0</p>

6272
4
AGARD

NATO  OTAN

7 RUE ANCELLE · 92200 NEUILLY-SUR-SEINE
FRANCE

Telephone 745.08.10 · Telex 610176

**DISTRIBUTION OF UNCLASSIFIED
AGARD PUBLICATIONS**

AGARD does NOT hold stocks of AGARD publications at the above address for general distribution. Initial distribution of AGARD publications is made to AGARD Member Nations through the following National Distribution Centres. Further copies are sometimes available from these Centres, but if not may be purchased in Microfiche or Photocopy form from the Purchase Agencies listed below.

NATIONAL DISTRIBUTION CENTRES

BELGIUM

Coordonnateur AGARD – VSL
Etat-Major de la Force Aérienne
Quartier Reine Elisabeth
Rue d'Evere, 1140 Bruxelles

CANADA

Defence Scientific Information Service
Department of National Defence
Ottawa, Ontario K1A 0Z2

DENMARK

Danish Defence Research Board
Østerbrogades Kaserne
Copenhagen Ø

FRANCE

O.N.E.R.A. (Direction)
29 Avenue de la Division Leclerc
92 Châtillon sous Bagneux

GERMANY

Zentralstelle für Luft- und Raumfahrt-
dokumentation und -information
c/o Fachinformationszentrum Energie,
Physik, Mathematik GmbH
Kernforschungszentrum
7514 Eggenstein-Leopoldshafen 2

GREECE

Hellenic Air Force General Staff
Research and Development Directorate
Holargos, Athens, Greece

ICELAND

Director of Aviation
c/o Flugrad
Reykjavik

UNITED STATES

National Aeronautics and Space Administration (NASA)
Langley Field, Virginia 23365
Attn: Report Distribution and Storage Unit

THE UNITED STATES NATIONAL DISTRIBUTION CENTRE (NASA) DOES NOT HOLD
STOCKS OF AGARD PUBLICATIONS, AND APPLICATIONS FOR COPIES SHOULD BE MADE
DIRECT TO THE NATIONAL TECHNICAL INFORMATION SERVICE (NTIS) AT THE ADDRESS BELOW.

PURCHASE AGENCIES

Microfiche or Photocopy

National Technical
Information Service (NTIS)
5285 Port Royal Road
Springfield
Virginia 22161, USA

Microfiche

Space Documentation Service
European Space Agency
10, rue Mario Nikis
75015 Paris, France

Microfiche

Technology Reports
Centre (DTI)
Station Square House
St. Mary Cray
Orpington, Kent BR5 3RF
England

Requests for microfiche or photocopies of AGARD documents should include the AGARD serial number, title, author or editor, and publication date. Requests to NTIS should include the NASA accession report number. Full bibliographical references and abstracts of AGARD publications are given in the following journals:

Scientific and Technical Aerospace Reports (STAR)
published by NASA Scientific and Technical
Information Facility
Post Office Box 8757
Baltimore/Washington International Airport
Maryland 21240, USA

Government Reports Announcements (GRA)
published by the National Technical
Information Services, Springfield
Virginia 22161, USA



Printed by Technical Editing and Reproduction Ltd
Harford House, 7-9 Charlotte St, London W1P 1HD

ISBN 92-835-1329-0